NETGEAR

Everybody's connecting.

FVL328 Cable/DSL ProSafe High-Speed VPN Firewall

Frequently Asked Questions

1. **What is the FVL328 Cable/DSL ProSafe High Speed VPN Firewall?**
   FVL328 is a network security device used to connect a Local Area network (LAN) securely via a broadband Internet connection to many other private LANs or individual remote users. It can also be used as a standalone firewall behind an existing router. The product provides 100 VPN tunnels and Stateful Packet Inspection (SPI) true firewall functionality.

2. **Is the FVL328 a router?**
   Yes, it is a router and much more. The FVL328 provides all the functionality of a Network Address Translation (NAT) router, plus many more security features.

3. **What is significant about the FVL328?**
   FVL328 provides additional security to the network in that it provides five significant features that do not exist in conventional NAT routers:
   - 100 tunnel VPN End point support with IPSec 3DES encryption capability
   - Static content filtering (URL, URL keywords)
   - Denial of Service (DoS) prevention through Stateful Packet Inspection
   - Logging, reporting and alerts (Intrusion Detection System)
   - Greatly increased performance using a high-speed CPU

4. **What is the difference between the FVL328 and NETGEAR's previously shipping FVS318?**
   The FVL328 has new features that provide better performance and functionality than the FVS318. Specifically, the FVL328 has:
   - Better WAN-to-LAN throughput (50+Mbps)
   - Support for 100 hardware-encrypted VPN tunnels (FVS318 has support for 8 software encrypted tunnels)
   - Better 3DES VPN tunneling throughput (15Mbps)
   - One of the lowest prices-per-port of any comparable VPN router product in the industry
   - A wider array of compatibility with other VPN products on the market, as demonstrated in testing by the VPN Consortium

5. **What is Virtual Private Networking?**
   Commonly known as a VPN and defined differently by different entities, it is a group of two or more computer systems, typically connected to a private network (a network built and maintained by an organization solely for its own use) with limited public-network access, that communicates "securely" (via a VPN "tunnel") over a public network, such as the Internet. VPNs may exist between an individual machine and a private network (client-to-server) or a remote LAN and a private network (server-to-server). Security features differ from product to product, but most security experts agree that VPNs include encryption, strong authentication of remote users or hosts, and mechanisms for hiding or masking information about the private network topology from potential attackers on the public network.

6. **What is VPN end point, and what can it do?**
   VPN end point capability within a router provides the ability to initiate a VPN tunnel to some other location that supports either a VPN client (client-to-box) or has VPN end point capability (box-to-box).

7. How many VPN tunnels can the FVL328 support at one time?

As a standard feature, the FVL328 has the ability to support up to 100 VPN tunnels at one time. This can be a combination of branch office, mobile users or partner connections.

8. What is encryption?

A mathematical operation that transforms data from "clear text" to "cipher text," which cannot be interpreted. Usually the mathematical operation requires that an alphanumeric key be supplied along with the clear text. The key and clear text are processed by the encryption operation, which leads to data scrambling that makes it secure. Decryption is the opposite of encryption; it is the mathematical operation that transforms cipher text to clear text.

9. How is the data encrypted on the FVL328 VPN?

The data is hardware-encrypted through the embedded encryption accelerator in the microprocessor.

10. What is DES and 3DES?

DES, or Digital Encryption Standard, is encryption used for data communications where both the sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. NETGEAR DES encryption uses a 56-bit key. 3DES, or "triple DES" on the other hand, is a variation on DES that uses a 168-bit key to provide more secure data transmission than DES. TripleDES is considered to be virtually unbreakable by security experts. It also requires a great deal more processing power, resulting in increased latency and decreased throughput unless hardware acceleration is provided, as in the FVL328.

11. What is IPSec?

Internet Protocol Security is a robust VPN standard that covers authentication and encryption of data traffic over the Internet. IPSec employs three components, encapsulating security payload (ESP), authentication header (AH), and Internet key exchange (IKE) technology. VPN technology employing IPSec will encrypt all outgoing data and decrypt all incoming data so that a public network can be used, like the internet, as transportation media. IPSec can support two encryption modes: transport and tunnel. Transport mode encrypts the data portion of each packet but leaves the header unencrypted. The more secure the tunnel mode encrypts both the header and the data. The FVL328 supports both. At the receiving end, an IPSec-compliant device decrypts each packet. For IPSec to work, the sending and receiving devices must share a key. IKE protocol is a key management protocol standard which is commonly used in conjunction with the IPSec standard. Unlike PPTP, IPSec is specific only to the Internet Protocol (IP) and does not provide security for other protocols. PPTP supports multiple protocols, but is not as secure.

12. What is IKE?

Internet Key Exchange is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE security association (SA) automatically negotiates encryption and authentication keys. With IKE, and initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass IP traffic.

13. What is Authentication Header (AH)?

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched. Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In

addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

14. What is Encapsulating Security Payload (ESP)?

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

15. What is a Security Association?

A group of security settings related to a specific VPN tunnel. A Security Association (SA) groups together all the necessary settings needed to create a VPN tunnel. Different SAs may be created to connect branch offices, allow secure remote management, and pass unsupported traffic. All SAs require a specified encryption method, IPSec gateway address and destination network address.

16. What is PKI?

Public Key Infrastructure (PKI) is a method by which valid VPN users are authenticated through the use of certificate authorities.

17. What is a Certificate Authority (CA)?

A Certificate Authority is an organization that provides certificates and provides a mechanism for verifying their authenticity. Certificate authentication is a method whereby the computer would have a pre-assigned certificate (any X.503-based certificate, such as Entrust®, VeriSign®, Baltimore, etc.) that is necessary for the IPSec-based authentication algorithm to use for generating keys to exchange between the two VPN devices. It is generally recognized as a more secure method of authentication.

18. What is PPTP?

Point-to-point Tunneling Protocol builds on the functionality of the Point-to-Point protocol (PPP) to provide remote access that can be tunneled though the Internet to a destination site or computer. PPTP encapsulates PPP packets using generic routing encapsulation (GRE) protocol, which gives PPTP the flexibility of handling protocols other than IP. The FVL328 supports pass-through mode for PPTP, but does not support end-point mode.

19. Why do need a router or firewall when I have a connection to the Internet through my PC already?

With the advent of computer hacking into homes and businesses, the increased reliance on home computers to store valuable information, and the development of applications that share content over the Internet through networked PCs, network security becomes an important issue. Simply connecting a PC to a DSL or cable modem does not provide the necessary security to prevent someone from hacking into a computer. Having a box that provides firewall or network address translation (NAT) capability provides a simple solution to this problem.

20. What is network address translation (NAT)?

NAT is used in the router to prevent hacking into the local area network (LAN). NAT substitutes the "private" IP address of devices located on the LAN side of the router with a new "public" IP address that is visible on the "Internet side" of the router. By virtue of this simple implementation, any device, up to 253, located on the LAN will be hidden, or "masqueraded" from Internet hackers trying to get to a specific PC. Only the router's IP address is visible on the Internet. This technology provides crude protection against hackers and is used widely in broadband routers.

21. Is this the same as a firewall?

No. Though the term "firewall" has been used generically when describing a router's ability to masquerade the PC's IP address, a true firewall employs a technology called Stateful Packet Inspection (SPI). Firewalls provide a greater level of security, and as a result, are generally more expensive than a NAT router. Firewalls give the administrator the ability to set up specific IP addresses or domain names that are allowed to be accessed while refusing the rest (filtering). Firewalls can also allow remote access to the private network through the use of secure login procedures and authentication certificates (Virtual Private Networks, or VPNs). Firewalls are used to prevent Denial of Service (DoS) attacks and can use software to provide content filtering to deny access to unwanted web sites. There are also extensive reporting capabilities, known as an Intrusion Detection System. The FVL328 and its siblings, the FV318, FR314 and FR318 are true firewalls.

22. What is Stateful Packet Inspection (SPI)?

SPI is a technology used in firewalls which instead of simply hiding an IP address from the Internet, will look at each individual packet for information such as its source and destination addresses and the protocol that is being used, in order to take certain actions based upon a set of pre-established criteria. SPI can be used to prevent DoS attacks, since the contents within the packet are known.

23. Can I turn off the NAT function on the router and use it just as a firewall behind the router that I already have?

The FVL328 will have this functionality in version 1.1 of the firmware, and will provide the ability to be used as simply a firewall/VPN device. It will also provide the ability to support static routes in order to set up subnets for larger scale networks.

24. What are Denial of Service (DoS) attacks?

Packets or requests for service sent from one or multiple PCs that cause disruption of functionality in the target PC or server. One way to employ a DoS would be to relentlessly "ping" the target server (known as "Ping of Death"), which requires the target server to respond to the ping. If there were enough pings requested, the unfortunate server would not be able to respond quickly enough to the pings and at the same time perform other functions. The result is a denial of service.

25. How does SPI prevent "Ping of Death" or SYN Flood DoS attacks?

The router will look at each packet and if the router notices a specific amount of ping requests over a certain amount of time coming from the same address, the packets will be dropped. In another example, the router

will know if the source address that is being sent is from within the LAN or external to the LAN. If an attack were launched from the WAN and an internal source address was used in the offending packet, normal routers would slow down, as they would not be able to tell where to respond. SPI-based routers are able to compare the "state" of the packet relative to previous packets and determine that the source address is incorrect, and therefore the offending packet would be dropped, thereby avoiding a slow down on the network.

26. What are the types DoS attacks?

- Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.
- Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAN Attacks.
- Brute-force attacks that flood a network with useless data such as Smurf attack.
- IP Spoofing

27. What other security functions do I get with the FVL328?

Along with true firewall functionality, the FVL328 also comes with Freedom® Anti-virus and privacy software from Zero Knowledge Systems. This complete, one-year subscription service is free with the purchase of the FVL328. The software can be used on up to 8 PCs on the LAN. There are other upgrades that are available if you have more than 8 PCs, or wish to take advantage of other security functionality offered by ZKS. See www.netgear.com for details.

28. What is content filtering?

It is the ability of the router to deny users access to a web site based upon a pre-determined set of rules. Content filtering can be done in a number of ways. Some of the more popular ways include filtering based upon the web page URL, key words within the URL and based upon the time of day and day of the week.

29. Does the FVL328 filter content this way?

Yes. These are included as standard features. This type of filtering is known as "static content filtering."

30. How many users does the FVL328 support?

The FVL328 supports up to 253 users in NAT mode, and can support more when NAT is turned off.

31. Where can I buy this product?

The FVL328 Cable/DSL VPN Router will be available in the major stocking distributors beginning mid December, 2002.

32. What kind of processor is used in the FVL328?

The FVL328 uses a 150Mhz MIPS32 processor.

33. How much memory does the FVL328 have?

The FVL328 has 2Mb of flash and 16Mb of DRAM memory on board, giving the user plenty of room to upgrade future functionality.

34. What other products do I need to purchase to use with the FVL328?

To use the FVL328, you will need to have an Ethernet Adapter and High Speed Broadband Internet connection (i.e.: Cable or DSL). Since the FVL328 has a 100Mbps WAN port, you can also use this with other devices, such as routers with 100Mbps connections.

35. How about if I want to establish 1 VPN tunnel to another site?

To establish a VPN tunnel, you'll need the following:

- A device that can establish a VPN tunnel, such as an FVL328 at the main office
- Either client software for the mobile user, or another device that can terminate the VPN tunnel, such as another FVL328. You can also use a router that supports IPSec pass-through used in conjunction with the client software (for secure connection-sharing at the remote site).

36. What if I need multiple-site VPNs?

Use the above rules for multiple sites, using the same client software or firewall router for each.

37. What VPN client software is supported on the FVL328?

The FVL328 supports the Safenet SoftRemote client, available at www.safenet-inc.com.

38. What about other VPN clients?

NETGEAR will provide application notes for set-ups of other VPN clients (such as Microsoft®, Nortel®, CheckPoint®, etc.) once testing and compatibility have been established and completed, and they will be available at the NETGEAR support site. These clients will not be supported as part of the standard technical support service, but support can be purchased on a "per incident" or "per minute" basis. See the details at www.netgear.com under the "technical support" section.

39. What about other VPN hardware devices?

NETGEAR FVL328 has been tested to be compatible with other FVL328s and will be supported through the technical support site. Much like the VPN software clients, application notes will be posted on the technical support site for other VPN hardware devices but will not be part of the standard technical support service. However, support can be purchased on a "per incident" or "per minute" basis. See the details at www.netgear.com under the "technical support" section.

40. What VPN products are compatible with FVL328?

- NETGEAR FVS318 ProSafe VPN Firewall Router
- FVL328 has also been tested through the VPN Consortium (VPNC), an independent member-supported entity to be compatible with the following:
  a. Adtran
  b. Ashley Laurent Broadway
  c. Asita VPN
  d. CheckPoint VPN-1
  e. Cisco IOS
  f. Cyberguard
  g. E-Soft Instagate
  h. NetBSD
  i. NetScreen 5XP OS3 and OS4
  j. OpenBSD
  k. SSH QuickSec
- The FVL328's VPN operating system (O/S) has been verified by ICSA (certification 1.0b) for interoperability for the following

a.	Furukawa Electric Company	InfoNet VP100
b.	Furukawa Electric Company	MUCHO EV/PK
c.	Lucent Technologies	Lucent VPN Firewall
d.	NetScreen Technologies	NetScreen 100
e.	Network Associates	Gauntlet VPN for HP-UX

f.	Network Associates	Gauntlet VPN for Solaris
g.	Network Associates	PGP 300 for Solaris
h.	Nortel Networks	Contivity Extranet Switch 1600
i.	Safenet	SafeNet / Soft-PK client
j.	Secure Computing	Sidewinder
k.	Symantec Corporation	Symantec Enterprise VPN (SEVPN)

41. What about backward compatibility with the FR318 and FV318?

You cannot set up a box-to-box VPN tunnel with the older FV318 and FR318, due to firmware limitations on the older devices.

42. Can I use another VPN router at the remote site in order to get more VPN tunnels to other locations?

This technique, known as a “hub and spoke” VPN method, is supported. This allows for a “mesh” topology between many sites.

43. What platforms does the FVL328 support?

For the routing portion, the FVL328 can be used on platforms (such as Macintosh®, Linux®, UNIX®, etc.) that employ the TCP/IP protocol and can use a browser (such as Netscape® and Microsoft Internet Explorer).

44. Will the FVL328 work with other LAN networking products beside NETGEAR?

The FVL328 will work with other networking products beside NETGEAR if these products are using Ethernet Standards (802.3).

45. How easy is it to connect to the Internet using the FVL328?

You can setup the FVL328 using your existing web browser (i.e.: Netscape or Internet Explorer). Simply connect your Cable/DSL modem to the WAN port on the back of the FVL328, connect the rest of computer(s) to the LAN ports, then configure the FVL328 by typing "192.168.0.1" at the URL address line on your Web browser. After logging in, launch the Smart Wizard and follow the instructions. Please refer to the manual for complete information.

46. I already have a 10 or 100Mbps Ethernet card, is it compatible with the FVL328?

Yes, the FVL328 has a built-in 10/100Mbps Auto-sensing switch which supports both 10 and 100Mbps.

47. The FVL328 supports “Auto Uplink™.” What is “Auto Uplink”?

Auto Uplink provides the ability for the LAN ports on the firewall to detect the correct connection requirements (either MDI or MDI-X) when connecting to other LAN devices, such as hubs or switches. By virtue of this functionality, it eliminates the need for cross-over cables and physical “uplink switches” on the device and makes connecting to other devices easier.

48. Does the FVL328 work with my current Cable or DSL Internet Service?

The FVL328 should work with most Cable or DSL Internet Service Providers. Your modem must have an Ethernet port to connect to the router.

49. What is the difference between static IP and dynamic IP addressing?

Static IP address is an IP address that is "permanently" assigned to the subscribers when they first sign up for their Internet Service. Dynamically allocated IP address is assigned to you temporarily when you connect to the Internet. The address has a pre-determined time limit.

50. How can I play Internet games (i.e.: Ages of Empire®, Quake®, Unreal Tournament®, etc…) and applications (i.e.: Napster®, ICQ®, AOL® Instant Messenger™, etc…:) with the FVL328?

Enable the public servers (inbound rules) feature of the web configuration screen. Generally, VPN products aren't recommended for "gamers," since the level of security, the processing required for the secure connections, and the encryption generally slows down the throughput, and may have adverse effects on the response time.

51. Does the FVL328 support a "DMZ"?

Yes, the FVL328 supports an exposed host, otherwise know as "DMZ." This allows you to set a device, such as a web server or PC used for games, outside the firewall. Refer to the manual for details. The FVL328 does not have a hardware DMZ port.

52. I am not able to get to the web configuration screen for the FVL328. What can I do?

- You may have to remove proxy settings on your Internet browser (i.e.: Netscape or Internet Explorer). Or, remove the dial-up settings on your browser
- The PC may not have received an IP address. Restart the PC or run the "winipcfg" utility (Windows ME or earlier, or "Ipconfig" utility on Windows NT platforms) to dynamically assign the IP address, and then launch the browser.

53. What is PPPoE?

PPPoE (Point to Point Protocol over Ethernet) is an informational RFC (2516) from the PPP working group of IETF. PPPoE is a much simpler way of supporting PPP over DSL accesses for Ethernet attached DSL modems. It takes advantage of Ethernet's shared environment along with PPP's familiar and secure dial-access user model. Other benefits to PPPoE include:

- Taking advantage of Ethernet's shared environments
- Allows for a single PC to set up PPP sessions to different destination networks at one time
- Enables a shared LAN and multiple PC's to simultaneously establish PPP sessions to different destination networks

54. Does the FVL328 support VPN other than through VPN end-point capability?

Yes, the FVL328 supports VPN passively through IPSec and PPTP pass-through.

55. Does the FVL328 support secure remote management?

Yes, secure remote management can be done via the web, using the SSL security of your browser. In addition, you can set up remote management to allow for anyone, a particular range of IP addresses, or only a specific IP address to remotely manage the device. Be sure to pick a good password for this function.

56. What is Secure Sockets Layer (SSL) functionality and does the FVL328 support on the remote management portion of the router?

A method of encryption of data sent through a web browser, SSL prevents someone from "sniffing" the HTTP transaction when the administrator is accessing the remote management portion of the router. This is a popular method used when making credit card transactions over the World Wide Web, and indicated by the "https:" in the address of the browser and the locked "padlock" icon in the browser's status bar.

57. Does the FVL328 support IPX or AppleTalk?

No, the FVL328 does not support IPX or AppleTalk.

58. Does the FVL328 support NetBEUI?

No, the FVL328 does not support NetBEUI.

59. Does the FVL328 support any Operating System?
Yes, the FVL328 is compatible with other Operating System provided the system supports TCP/IP (i.e. can support a web browser).

60. How do I set restriction on what web sites my employees are allow to view?
You can use the "content filtering" page on the FVL328 to setup these options. Please refer to the FVL328 manual for a more complete description of how to set up the FVL328.

61. Can I change the factory default password?
Yes you can, please refer to the User Manual for more information on changing these parameters.

62. How do I check to see if my ports are secured?
You can check by using a third party scanning utility (i.e.: http://www.grc.com or www.sygatetech.com).

63. How do I contact Technical Support?
You can contact NETGEAR Technical Support by:

- Call 1-888-NETGEAR (638-4327)
- Email: support@NETGEAR.com

64. How do I find out more about VPN?
Check out www.netgear.com and click on the “PlanetVPN” tab in the Firewall/VPN routers section.